

Express Mail Label No.: EV 292 547 997 US

DOCKET NO: S01022.81054.US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Pierre-Yvan LIARDET, Fabrice ROMAIN, Yannick
TEGLIA, and Laurence SIRTORI
Serial No: Unassigned
Confirmation No: Unassigned
Filed: Herewith
For: CYPHERING/DECYPHERING PERFORMED BY AN
INTEGRATED CIRCUIT

Examiner: Unassigned
Art Unit: Unassigned

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

PRELIMINARY AMENDMENT

Prior to examination on the merits of the application, please amend the above-identified application as follows:

IN THE ABSTRACT

Please amend the Abstract as shown below:

A method of cyphering and/or decyphering, by an integrated circuit, of a digital input code by means of several keys, ~~consisting of~~ comprising: dividing ~~said~~ the code into several data blocks of same dimensions; and applying to said blocks several turns of a cyphering or decyphering ~~consisting of~~ comprising submitting each block to at least one same non-linear transformation and of subsequently combining each block with a different key at each turn, the operands being masked, upon execution of the method, by ~~means of~~ at least one first random number having the size of ~~said~~ the code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.